Preventing Charity Cybercrime

Insights+Action

OCTOBER 2019

FRAUD ADVISORY PANEL

CHARITY COMMISSION FOR ENGLAND AND WALES

58%

of charities think cybercrime is a major risk to the charity sector

22%

believe cybercrime is a greater risk to the charity sector than other sectors

Preventing Charity Cybercrime

Cybercrime is a rapidly growing threat to the charity sector, causing direct harm to charities and beneficiaries alike. Everyone has a part to play in tackling this problem. The Charity Commission for England and Wales, together with government partner, the National Cyber Security Centre, is committed to helping charities address this threat by giving them the understanding and tools they need to combat cybercrime. Public trust and confidence in the sector relies upon good governance in charities, and ensuring effective cyber security is a vital component.

Insights+Action

Preventing Charity Cybercrime

Research insights

This report highlights the main findings from our cybercrime survey of registered charities in England and Wales during March 2019. The Commission, supported by the Fraud Advisory Panel, contacted a representative and randomly selected sample of 15,000 charities, achieving a 22% response rate.

The results represent the largest survey ever undertaken into cybercrime in the UK charity sector, and provide insights into the threats facing the sector and the actions required to combat them.

Trends in tackling charity cybercrime

The initial results of the survey are encouraging, with many charities managing the risk well, but there's more that can be done.

- In the next two years, one in every six large charities will suffer from cybercrime. Many other charities will be the victim of cyber-attacks without knowing about it. **Protect your charity in case it's next.**
- Charities who have suffered cybercrime go on to revise their IT security, their training programmes or their website security. **Make those changes before you charity is affected.**
- A charity is four times more likely to discover cybercrime through internal IT controls or by staff raising concerns than all other external sources combined. **Strengthen your controls rather than relying on others.**
- The biggest impacts of cybercrime are financial loss and data loss. **Protect yourself from the risk.**

Scale and level of cybercrime

Charities in England and Wales spend nearly £80 billion of valuable funds per year. They hold financial and personal information that cyber criminals increasingly target, though there's no definitive estimate of the scale of cybercrime facing the sector. Some larger charities believe they experience several thousand attempted cyber-attacks every week. Encouragingly, most are prevented by the application of robust defences, such as up-to-date software patching and firewalls, combined with the vigilance of charity staff.

It's likely that limited access to expertise and a relative lack of resources, especially for smaller charities, is having a detrimental effect on the cyber resilience of the sector.

Trustees, who bring a wealth of varied knowledge and experience to charities, have a higher age profile (65-74 years on average for smaller charities) than the general public. Research suggests that higher age groups can have lower levels of cyber awareness and technical skills, potentially making them more vulnerable to cybercrime.

Taken in combination this suggests that parts of the charity sector, particularly smaller charities, could be more vulnerable to cybercrime than equivalent size organisations in the private or public sectors.

Helpful definitions

Cybercrime: An umbrella term for many different types of crime, which occur either online or where technology is a means and/or a target for the attack.

Phishing/Malicious emails: Using hoax emails to trick recipients into revealing sensitive information.

Hacking/Extortion: Hacking is a general term used to describe unauthorised access to someone else's computer.

Distributed Denial of Service (DDoS) attack: an attack launched on a system by a network of computers, called a botnet, which causes disruption to a computer or website.

Perception of risk

- More than half (58%) of charities think cybercrime is a major risk to the charity sector
- Almost a quarter (22%) believe cybercrime is a greater risk to the charity sector than other sectors
- Larger charities are generally more likely to appreciate the risk of cybercrime.

CONCLUSION

Charities are increasingly aware of the risk of cybercrime, with larger charities more likely to appreciate the threat. This may be because larger charities generally have a greater capability to detect cybercrime. Many small and medium sized charities are less aware of the cybercrime threat, yet are probably more at risk.

ACTION

CHARITIES SHOULD ACKNOWLEDGE THE SUBSTANTIAL THREAT OF CYBERCRIME AND UNDERSTAND THE HARM IT CAN CAUSE THEIR CHARITY.

Managing the risk

- Charities see phishing and malicious emails as the greatest cyber threat (39%), followed by hacking/extortion (15%) and Distributed Denial of Service (DDoS) attacks (2%)

- Over a third (36%) of charities don't know which type of cyber-attacks they're most vulnerable to

- Nearly half of charities state that the Board has overall responsibility for cyber security, whilst 15% state nobody has responsibility. For the remainder, nominated Trustees, Chief Executives, or IT and Finance Directors have this responsibility.

CONCLUSION

Phishing and malicious emails are perceived to be the main cyber threat. In most charities the overall responsibility for cyber security sits predominantly with the Board.

ACTION

CHARITIES SHOULD CLARIFY RESPONSIBILITY FOR MANAGING THE RISK OF CYBERCRIME AND ENSURE IT'S A GOVERNANCE PRIORITY FOR THE BOARD.

Frequency of cybercrime

(these results relate only to where a cybercrime has occurred in the last 2 years)

- 3% of charities are known to have suffered a successful cyber-attack in the past two years, with large charities far more likely to have been victims. It's likely that many other cyber-attacks have gone undetected

- Where a cyber-attack has occurred, the most common types were phishing/malicious emails (54%) and hacking/extortion (31%).

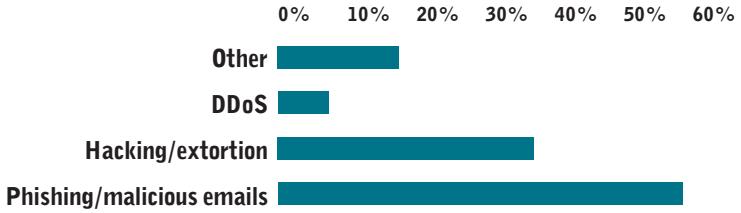
CONCLUSION

Large charities are more likely than smaller charities to be the victim of a cybercrime with phishing/ malicious emails the most common method of attack. The high volume of such attacks means that virtually any organisation can fall victim. Smaller charities remain a target.

ACTION

CHARITIES SHOULD RAISE AWARENESS OF CYBERCRIME AND ENCOURAGE TRUSTEES, STAFF AND VOLUNTEERS TO RAISE CONCERNS, ESPECIALLY WHERE PHISHING ATTACKS AND MALICIOUS EMAILS ARE SUSPECTED.

Types of charity cyber-attacks in the last two years



MORE THAN TWO

THIRDS

of charities took action to strengthen their defences after a cyber-attack

NEARLY

HALF

of charities state that the Board has overall responsibility for cyber security

Identification and reporting

(these results relate only to where a cybercrime has occurred in the last 2 years)

- Most cybercrime has been discovered through internal control arrangements, with almost a third (30%) identified by internal IT controls and over a quarter (26%) by staff raising a concern. By contrast 23% was discovered by accident and only 13% identified by a source external to the charity

- Reporting by charities remains low, with less than a third (29%) reporting cybercrimes to the police, a quarter to their bank and 13% to the Charity Commission. 32% did not report to any external body when they'd fallen victim

- 84% reported the cybercrime to the Board.

CONCLUSION

The effectiveness of internal arrangements, in particular IT controls, combined with the awareness of staff and volunteers, is critical in the speedy identification of cybercrime. Charities should not rely on accidental identification as a control. The high level of reporting to the Board is encouraging but more needs to be done to report to external agencies such as the police.

ACTION

SUCCESSFUL CYBER-ATTACKS SHOULD BE REPORTED TO THE BOARD AND TO APPROPRIATE EXTERNAL ORGANISATIONS, INCLUDING THE POLICE AND CHARITY COMMISSION.

The impact of cybercrime

(these results relate only to where a cybercrime has occurred in the last 2 years)

- Over a third (35%) of charities that suffered a cybercrime stated it had no impact on the charity

- Where there was an adverse impact, 19% reported financial loss, 15% data loss, 12% loss of time or other inconvenience, 10% reputational damage, and 9% limited their charitable activities as a result

- Only 1% reported adverse publicity following the cybercrime.

CONCLUSION

When a cyber-attack occurs it can have a significant impact on charities, potentially causing harm through loss of funds and sensitive data. Taking preventative action is cost effective in reducing the harm caused.

ACTION

CHARITIES SHOULD BE OPEN AND TRANSPARENT WHEN DEALING WITH CYBERCRIME, ADOPTING A PRO-ACTIVE APPROACH THAT PRIORITISES DETECTION AND PREVENTION.

Responding to cybercrime

(these results relate only to where a cybercrime has occurred in the last 2 years)

- Where a charity has been a victim of cybercrime, more than two thirds (69%) made changes as a result – 39% revised IT security arrangements, 25% provided new or updated training and 11% revised website security

- For those charities who thought that poor preventative measures contributed to the cybercrime, 13% noted poor risk management or controls, whilst 10% thought the charity was too trusting.

CONCLUSION

Encouragingly, two thirds of charities took action to strengthen their defences after a cyber-attack, with revised IT security arrangements and new or updated training the principal responses.

ACTION

CHARITIES SHOULD ACT EARLY AND REVIEW PREVENTION ARRANGEMENTS BEFORE A CYBERCRIME HAS OCCURRED.

36%

of charities don't know which type of cyber-attack they're most vulnerable to

84%
of charities reported the cybercrime to the Board

30%
of cybercrimes were identified by internal IT controls

JUST 29%
of charities reported cybercrimes to the police

Taking action

Trustees can self-assess their charity against the checklist at the end of this report, consider the case studies provided and use the good practice guidance available via the links below. Taking these simple steps will help improve knowledge levels and boost resilience. All charities, regardless of size and type, are encouraged to make an immediate impact by taking action now.

Guidance and further info

The National Cyber Security Centre and Charity Commission have worked together to develop resources relevant to charities of all sizes

Cyber Security: Small Charity Guide

This guide provides quick, simple, free/low-cost steps to improve cyber security.
www.ncsc.gov.uk/charity

The Board Toolkit

Relevant for larger charities, this guidance helps Boards and senior managers understand cyber security from a governance perspective, making it easier to have productive conversations with technical colleagues.
www.ncsc.gov.uk/collection/board-toolkit

10 Steps to Cyber Security

Guidance for IT teams and cyber security professionals. This guide breaks down the task of defending your networks, systems and information into its essential components, providing advice on how to achieve the best possible security for your charity in each of these areas.
www.ncsc.gov.uk/collection/10-steps-to-cyber-security

Cybercrime awareness day

Part of International Charity Fraud Awareness Week – each year a series of themed webinars and fact sheets is produced, aimed at boosting cyber resilience in the sector.
Visit the online hub
www.fraudadvisorypanel.org/charity-fraud/get-involved

Protect your charity from fraud and cybercrime

Hosted by the Charity Commission, these webpages feature best practice guidance from across government, professional organisations and the Charities Against Fraud Group
www.gov.uk/guidance/protect-your-charity-from-fraud

Charity Cybercrime Case Studies

CASE STUDY 1

Responding to multiple cyber-attacks

A charity was the subject of five successful malware attacks over a three month period. This included Wannacry ransomware, which exploited vulnerabilities in older non-supported operating systems, and a crypto-virus that entered the charity network using a remote access route.

Cybercriminals attempted to extort 30 Bitcoins from the charity, valued at that time at £186,000. The charity did not pay out, but instead undertook forensic IT activities to quantify the damage and put in place arrangements to mitigate the harm caused.

It was found that server backups had also been compromised. Although staff pay and other charity activities were affected for a three week period, no data breaches were identified.

CASE STUDY 2

Email account hacked and attempted mandate fraud

A charity worker had their email account hacked. A subsequent email sent by a legitimate partner charity was diverted by the hacker, adjusted with new bank account information and then forwarded on to the charity worker as originally intended. The adjusted email now requested that the charity make a £7,000 grant payment to a new bank account, controlled by the hacker, rather than the legitimate account of the partner charity. This is a type of cyber enabled mandate fraud.

Fortunately the charity worker was told that the email account had been hacked and had become suspicious of the email regarding change of bank details. The grant payment was not made. Subsequent checks confirmed that the email had been fraudulently altered. The charity worker took immediate steps to enhance controls by strengthening passwords used and installing a new hard drive on the computer.

CASE STUDY 3

Phishing attack

A large medical funding charity suffered two phishing attacks in a short period of time after fraudsters gained access to the email accounts of four senior officers of that charity. This occurred after the senior officers clicked on links in a hoax email, entering passwords which then allowed fraudsters access to sensitive information.

The police were contacted after the phishing attack was discovered and the incident reported to the Charity Commission and Information Commissioner's Office. Thanks to the immediate action that was taken there was no financial loss.

The charity has since taken steps to be more open and transparent about security breaches, including listing the phishing attack in their Annual Report. The charity also introduced a staff awareness training programme and hired a cyber-security specialist.

FRAUD ADVISORY PANEL

The Fraud Advisory Panel is the independent voice of the counter-fraud profession. It champions anti-fraud best practice and works to improve fraud awareness, understanding and resilience.
fraudadvisorypanel.org

CHARITY COMMISSION FOR ENGLAND AND WALES

The Charity Commission registers and regulates charities in England and Wales. It ensures that charities meet their legal requirements and provides guidance to help them run themselves as effectively as possible while also preventing abuse (including fraud).
gov.uk/government/organisations/charity-commission

Populus

Populus is a research & strategy consultancy and a trusted adviser to some of the UK's biggest businesses and most important organisations. We use research, evidence and expertise to provide clients with the critical knowledge they need to succeed. Our work helps organisations navigate the issues and audiences that make the difference between success and failure.
populus.co.uk

Cybercrime Prevention Checklist

For completion by charity trustees, staff and volunteers

ACTION	YES	PARTIALLY	NO	COMMENTS
1. Acknowledge the increasing threat from cybercrime and the harm it can cause.				
2. Clarify responsibility for managing the risk of cybercrime				
3. Raise awareness of the cyber threat and encourage trustees, staff and volunteers to raise concerns, especially regarding phishing attacks and malicious emails				
4. Report successful cyber-attacks to the Board and to appropriate external regulators, including the police and Charity Commission				
5. Aim to be open and transparent when dealing with cybercrime, adopting a pro-active approach that prioritises prevention arrangements				